

Information Security Oversight Office, NARA

§ 2004.5

(s) *Security-in-depth* means a determination by the agency head that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System (IDS), random guard patrols throughout the facility during nonworking hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during nonworking hours.

(t) *Supplemental controls* means prescribed procedures or systems that provide security control measures designed to augment the physical protection of classified information. Examples of supplemental controls include intrusion detection systems, periodic inspections of security containers or areas, and security-in-depth.

(u) *Temporary records* means Federal records approved by NARA for disposal, either immediately or after a specified retention period. Also called *disposable records*.

(v) *Transclassification* means information that has been removed from the Restricted Data category in order to carry out provisions of the National Security Act of 1947, as amended, and safeguarded under applicable Executive orders as "National Security Information."

(w) *Unscheduled records* means Federal records whose final disposition has not been approved by NARA. All records that fall under a NARA approved records control schedule are considered to be scheduled records.

PART 2003 [RESERVED]

PART 2004—NATIONAL INDUSTRIAL SECURITY PROGRAM DIRECTIVE NO. 1

Subpart A—Implementation and Oversight

Sec.

2004.5 Definitions.

2004.10 Responsibilities of the Director, Information Security Oversight Office (ISOO) [102(b)].

2004.11 Agency Implementing Regulations, Internal Rules, or Guidelines [102(b)(3)].

2004.12 Reviews by ISOO [102(b)(4)].

Subpart B—Operations

2004.20 National Industrial Security Program Operating Manual (NISPOM) [201(a)].

2004.21 Protection of Classified Information [201(e)].

2004.22 Operational Responsibilities [202(a)].

2004.23 Cost Reports [203(d)].

2004.24 Definitions.

AUTHORITY: Executive Order 12829, January 6, 1993, 58 FR 3479, as amended by Executive Order 12885, December 14, 1993, 58 FR 65863.

SOURCE: 71 FR 18007, Apr. 10, 2006, unless otherwise noted.

Subpart A—Implementation and Oversight

§ 2004.5 Definitions.

(a) "Cognizant Security Agencies (CSAs)" means the Executive Branch departments and agencies authorized in EO 12829, as amended, to establish industrial security programs: The Department of Defense, designated as the Executive Agent; the Department of Energy; the Nuclear Regulatory Commission; and the Central Intelligence Agency.

(b) "Cognizant Security Office (CSO)" means the organizational entity delegated by the Head of a CSA to administer industrial security on behalf of the CSA.

(c) "Contractor" means any industrial, education, commercial, or other entity, to include licensees or grantees that has been granted access to classified information. Contractor does not include individuals engaged under personal services contracts.

(d) "National Interest Determination (NID)" means a determination that access to proscribed information is consistent with the national security interests of the United States.

(e) "Proscribed information" means Top Secret; Communications Security, except classified keys used for data

§ 2004.10

transfer; Restricted Data; Special Access Program; or Sensitive Compartmented Information.

[71 FR 18007, Apr. 10, 2006. Redesignated and amended at 75 FR 17306, Apr. 6, 2010]

§ 2004.10 Responsibilities of the Director, Information Security Oversight Office (ISOO) [102(b)].¹

The Director ISOO shall:

- (a) Implement EO 12829, as amended.
- (b) Ensure that the NISP is operated as a single, integrated program across the Executive Branch of the Federal Government; i.e., that the Executive Branch departments and agencies adhere to NISP principles.
- (c) Ensure that each contractor's implementation of the NISP is overseen by a single Cognizant Security Authority (CSA), based on a preponderance of classified contracts per agreement by the CSAs.
- (d) Ensure that all Executive Branch departments and agencies that contract for classified work have included the Security Requirements clause, 52.204-2, from the Federal Acquisition Regulation (FAR), or an equivalent clause, in such contract.
- (e) Ensure that those Executive Branch departments and agencies for which the Department of Defense (DoD) serves as the CSA have entered into agreements with the DoD that establish the terms of the Secretary's responsibilities on behalf of those agency heads.

§ 2004.11 Agency Implementing Regulations, Internal Rules, or Guidelines [102(b)(3)].

(a) *Reviews and Updates.* All implementing regulations, internal rules, or guidelines that pertain to the NISP shall be reviewed and updated by the originating agency, as circumstances require. If a change in national policy necessitates a change in agency implementing regulations, internal rules, or guidelines that pertain to the NISP, the agency shall promptly issue revisions.

(b) *Reviews by ISOO.* The Director, ISOO, shall review agency imple-

¹Bracketed references pertain to related sections of Executive Order 12829, as amended by E.O. 12885.

32 CFR Ch. XX (7–1–10 Edition)

menting regulations, internal rules, or guidelines, as necessary, to ensure consistency with NISP policies and procedures. Such reviews should normally occur during routine oversight visits, when there is indication of a problem that comes to the attention of the Director, ISOO, or after a change in national policy that impacts such regulations, rules, or guidelines. The Director, ISOO, shall provide findings from such reviews to the responsible department or agency.

§ 2004.12 Reviews by ISOO [102(b)(4)].

The Director, ISOO, shall fulfill his monitoring role based, in part, on information received from NISP Policy Advisory Committee (NISPPAC) members, from on-site reviews that ISOO conducts under the authority of EO 12829, as amended, and from complaints and suggestions from persons within or outside the Government. Findings shall be reported to the responsible department or agency.

Subpart B—Operations

§ 2004.20 National Industrial Security Program Operating Manual (NISPOM) [201(a)].

(a) The NISPOM applies to release of classified information during all phases of the contracting process.

(b) As a general rule, procedures for safeguarding classified information by contractors and recommendations for changes shall be addressed through the NISPOM coordination process that shall be facilitated by the Executive Agent. The Executive Agent shall address NISPOM issues that surface from industry, Executive Branch departments and agencies, or the NISPPAC. When consensus cannot be achieved through the NISPOM coordination process, the issue shall be raised to the NSC for resolution.

§ 2004.21 Protection of Classified Information [201(e)].

Procedures for the safeguarding of classified information by contractors are promulgated in the NISPOM. DoD, as the Executive Agent, shall use standards applicable to agencies as the basis for the requirements, restrictions, and safeguards contained in the